

An Efficient Buyer - Seller Protocol to Identify the Perpetrator

¹Vinu V Das, ²J. FazlurRahman

¹Faculty of Computer Science & Engineering, Pacific University, Udaipur, India

²Professor Emeritus & Head (R&D Centre), HKBK College of Engineering, Bangalore, India

Email: ¹vinuvdas@gmail.com, ²jfazlu2003@yahoo.co.in

Abstract: Digital watermarks are used to prevent the possession and transmission of copyright intellectual property over the internet. Digital watermarking system is playing an irrevocable role in privacy-preserving, buyer-seller communication and e-commerce of digital content. In the past, many buyer-seller protocols have been proposed to address the copyright issues. Most of these protocols are only protecting digital copyright of the digital content. This paper proposes a new efficient buyer seller watermarking protocol for secure digital transaction and to identify the Perpetrator who actually pirates the digital content. To implement this system we use a multi layer Terminate and Stay Resident (TSR) scripting programs before embedding the watermarking.

I. INTRODUCTION

The major benefit of digital revolution is the ease of communication and duplication of digital contents. Even though such benefits often create limitation to the copyright owners from having a financial gain from licensing such contents, digital watermarking has been prepared as a suitable deterrent to illegal copying and distribution.

A digital watermarking is an imperceptible information, regarding the copyright owner, embedded to degrade linearly with the degradation of the content itself. Embedding the watermark information into the digital content will help to identify the originality of the content as well as the copyright owner and buyer/dealer. Having a digital watermarking buyer-seller protocol for the privacy preservation and to trace piracy to the original perpetrator is the need of the day. Moreover the system may also provide a provision to buyers, sellers, owners or dealers to check the originality of the system.

In the past, many buyer-seller protocols have been proposed to address the copyright issues. Most of these protocols [6-13] are not only protecting digital copyright by embedding watermarking in digital content but also protecting the digital content.

In Poh and Martin's framework, the buyer generates the watermark and the watermarking authority is used to verify that the watermark is well formed such as [5] and [12]. My previous work [7] and [10] are addressing the issues of customer right's and unbinding problem. It also solves buyer verification and certification authority obligation problem.

William etl [14] introduced the concept of rigorous analysis of buyer-seller watermarking protocols using a formal analysis technique used to check communication protocols. All these system have miserably failed to identify the culprit if the embedded copyrighted watermarking content on the

digital content is changed or hacked.

Even though many solutions are proposed for many issues of privacy and buyer-seller with watermarking, no effort has made to identify the perpetrator of the piracy. Buyer-seller protocol in this paper is a novel method for protecting the privacy and locate the original perpetrator who actually pirated the digital content. The proposed system alerts the copyright owner regarding the geographical and network location of the perpetrator, as soon as privacy is encountered.

II. PROPOSED SYSTEM

The proposed protocol mainly address the issue to identify the perpetrator, as soon as privacy is encountered. The proposed model based on any public key cryptosystem has five different roles as follows.

1. **O:** The copyright owner of the licensed digital content, who wants to sell the product through the seller or dealer.
2. **S:** The seller or the sales point, from where the buyer purchases the digital content. The seller may be the original owner of the digital content, or an authorized reselling agent or dealer.
3. **B:** The genuine buyer, who wants to purchase a digital content from the seller S.
4. **H:** The present holder of the digital content who is processing the pirated watermarked content.
5. **CA:** The Watermark Certification Authority is responsible for issuing watermark based on Transaction Identification number (TID), Holder's MAC, Holder's Public key (Ps), and Product Identification number (PID). The WCA also issues the digital signature certificate based on private key in such a way that anyone in the electronics commerce transaction can check the authenticity to avoid any future repudiation. They may appoint trusted Regional Watermark Certification Authorities (RWCA) to share and reduce its workload.
6. **ARB:** An arbiter, who adjudicates lawsuits against the infringement of copyright and intellectual property.

This paper restricts itself to further discussion on security or implementation issues related to the public key cryptosystem by assuming that a public key infrastructure has been well deployed so that each party has its own public-private key pair as well as a digital signature certificate issued by WCA. Before elaborating further on the proposed protocol, the notations used in this model are defined below.

X	Original copy of the digital content
W	Generated Watermark, which is to be embedded into the digital content X
MAC	Media Access Control (MAC) address of the networking device is used for generating the watermarking. MAC is also used identify the perpetrator.
PID	Unique number given by the CA to identify a digital product, which will be published in website for anyone who is likely to take part in the transaction.
TID	The CA is responsible for issuing a unique random number for every transaction, in order to prevent the duplication when selling more copies of a digital content to a specific B by aSor O.
TSR	A kind of a Terminate and Stay Resident (TSR) scripting program that can access MAC of the system to compare the same in the watermarked content. No access to memory or processing or any other system unit. The TSR will active till the digital content is
WID	Watermark Identification number is generated by CA, which is only known to CA for verifying the originality of the purchased product. WID will be stored in a database along with TID, PID, B, S details.
$\oplus$	Watermark information binary insertion operator, which inserts watermark into the original copy of digital content.
X'	Watermarked digital content, where the watermark W is inserted into the digital content X using a function μ , $\mu(X \oplus W)$.
(P_s, S_s)	A public-secret key pair, where P_s is S's public key and S_s is S's secret key.
Public key encryption and decryption algorithms	
$E_{pb}(M)$	The message M is encrypted using B's public key
$D_{sca}(C)$	The cipher text C is decrypted using CA's private key

By $X \oplus W$ means, where $W = (W_s \otimes W_B)$

$$x_1 \oplus w_1, x_2 \oplus w_2, \dots, x_n \oplus w_n, x_{n+1} \oplus w_{n+1}, \dots, x_m \oplus w_m \}$$

A privacy homomorphism with respect to the binary operator $\oplus$ is applied to insert a watermark W to any original copy of the digital content X. For every a and b in the message block, $\oplus$ has the property that

$$E_{pk}(a \oplus b) = E_{pk}(a) \oplus E_{pk}(b)$$

where PK is the public encryption key. The buyer-seller protocol in this section, using watermark techniques for an efficient and secure digital transaction, has five sub-protocols: *Registration and Buyer-Seller Protocol*, *TSR Watermarking*, *Perpetrator Alert*, *Arbitration Protocol* and *Relocation Request*.

A. Registration and Buyer-Seller Protocol

Figure 1 shows the proposed registration protocol for any buyer-seller networking transaction using watermarking,

where the O registers a digital content, to be sold, with the Certification Authority (CA) with the Product ID number, PID. Once the O reaches to an agreement on the terms and conditions regarding price and service with the seller or dealer S, it will request the CA to issue the digital marked content to S with their Media Access Control address, MACo, and public key, Po for the a specific product transaction, TID.

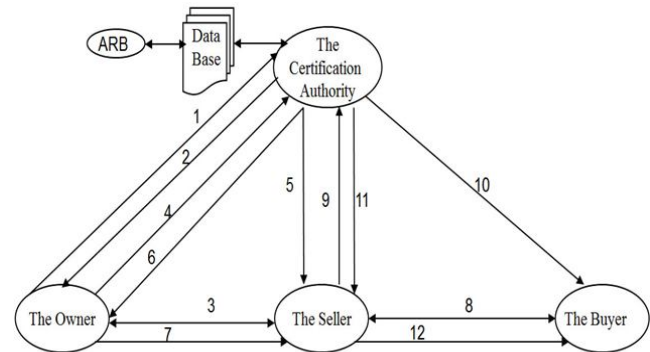


Fig. 1 Registration and Buyer-Seller protocol

Figure 2 has the details of possible transactions in the proposed registration and Buyer-Seller protocol, which is explained below:

1. When O wants to sell a digital content over an internet, first it has to register with CA with the product Identification number, PID, and the Public Key P_o . O initiates the registration transaction by sending an encrypted PID and P_o with CA's public key, $E_{pca}(PID + P_o)$.
2. CA generates the unique watermarking after collecting the MAC_o , P_o and Transaction identification number, TID. The this watermark is combined with the TSR scripting program

$$E_{p_o}[X \oplus TSR \oplus W(MAC_o, TID, P_o)]$$

All these details are stored in the CA's database, and it is only known to CA and corresponding arbitrator ARB.

3. O will identify, negotiate, and finalize the terms and conditions of the possible dealers, D or a Seller, S; to possibly identify the genuine Buyers, B.
 4. O will request CA to issue the watermarked content of PID to S. $E_{pca}(Ps, PID)$
 5. CA identifies the MAC of S and issues the watermarked content to S, for possible display and identification of the genuine Buyers, B
- $$E_{ps}[X \oplus TSR \oplus W(MAC_s, TID, Ps)]$$
6. CA sends the acknowledgement, $E_{p_o}[ACK(Ps, PID)]$, to O regarding the watermarked PID to S.
 7. O sends the acknowledgement, $E_{ps}[ACK(Ps, PID)]$, to S regarding the watermarked PID from CA.
 8. S will identify, negotiate, and finalize the payments with the genuine Buyers, B.
 9. S will request CA to issue the watermarked content of PID to B. $E_{pca}(Pb, PID)$
 10. CA identifies the MAC of B and issues the watermarked content to B.
- $$E_{pb}[X \oplus TSR \oplus W(MAC_b, TID, Pb)]$$
11. CA sends the acknowledgement, $E_{ps}[ACK(Pb, PID)]$, to

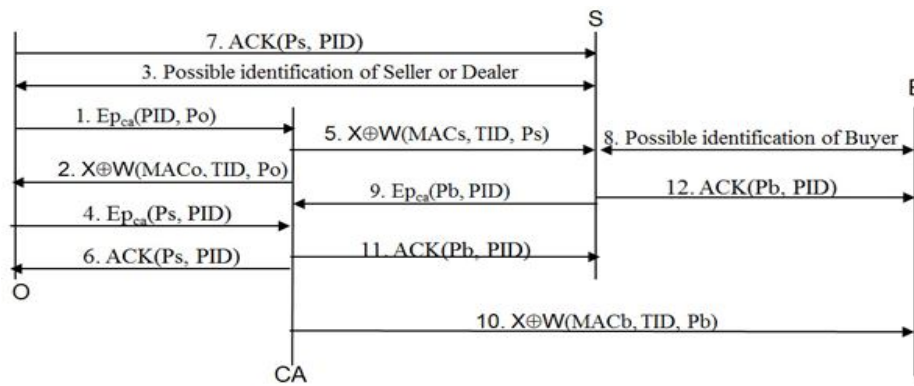


Fig. 2 Transactions in the Registration and Buyer-Seller Protocol

S regarding the watermarked PID to B.

12. S sends the acknowledgement, $E_{pb}[ACK(Pb, PID)]$, to B regarding the watermarked PID from CA.

At the end of the registration and buyer-seller protocol, S is authorized to sell the product **PID**, by **O**; and S identifies the buyer **B** to sell the watermarked product through **CA**.

B. TSR Watermarking

Figure 3 shows the TSR watermarking in 3 layers. The base layer is the actual digital content **X** to be sold. Layer 2 is the flag checking **TSR** scripting program, generated by the **CA**, which will contain encrypted static 10 flag counters (as shown in the Figure 4) to store the required information to check the piracy. The **TSR** (runs itself and checks in every minute or hour or day as the security of the content demands) will access the **MAC** of the existing place of digital content and check the flag of the digital content with the help of **KEY** and **P_H**. If anyone tries to duplicate the content the **CARRY** and **KEY** changes, and alert generates. If an unauthorized person is holding the content without duplicating, then the **P_H** (when decrypting the **S_H**) and **MAC** changes will be noticed. The system implementers have every freedom to design the Flag Counters to maximize the security.

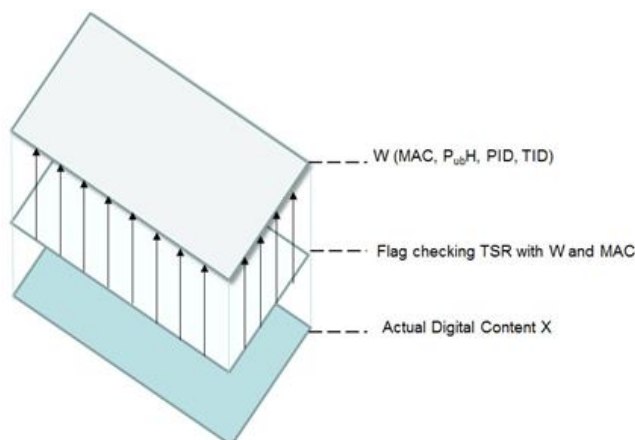


Fig. 3 TSR watermarking in 3 Layer

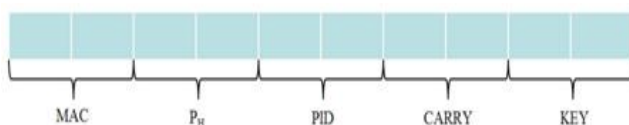


Fig. 4 Static Flag Counters in the TSR Layer

Third layer of the TSR watermarking is the actual watermark information where **P_H**, **PID** and other information is embedded to solve numerous other issues resolved till now.

C. Perpetrator Alert

The Figure 5 shows the Alert mechanism implanted in the watermarked content with the help of TSR, when a piracy is observed.

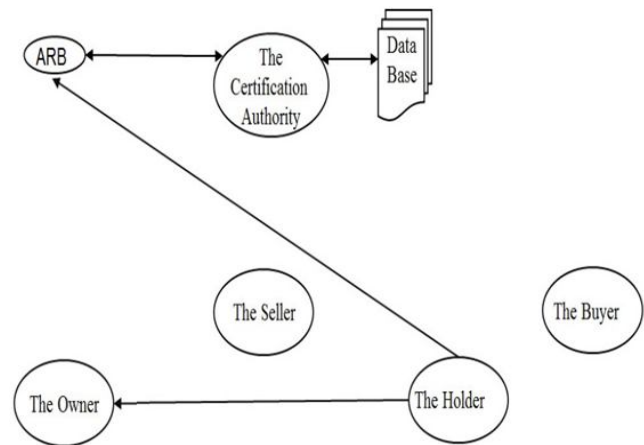


Fig. 5 Perpetrator Alert

Piracy can be detected in three cases by the **TSR** by looking at the flags, **MAC** and Watermarked contents. Case(1): where the holder, **H**, of the digital content is carrying the original digital content intended for another genuine buyer, **B**. **TSR** will detect this by checking the **MAC** of the holder. In this case **H** may not be able to use the digital content as **H** will not be able to decrypt using the **S_H**, and requires **S_B**. Case(2): where the holder, **H**, of the digital content is carrying the duplicate digital content. The **CARRY** and **KEY** flag might have changed when duplicating the content. Apart from that **MAC** and **P_B** will differ. Case(3): where the genuine buyer **B**, of the digital content duplicated the original content. **TSR** will identify and alert the **CARRY** and **KEY** flag which is changed when duplicating the content. The alert (IP and MAC address of the **H**, **PID**, **P_o**, **P_s**, **P_H**, **TID**) is often sent to the **O** of the digital content and **ARB**.

D. Arbitration Protocol

The information related to the licensed owner, **O**, and corresponding arbitrator, **ARB**, information is stored in the

watermark. Tampering this information will destroy (completely or partially) the digital content. As soon as piracy is observed, an alert is initiated to the **O** of the digital content and **ARB**. The **ARB** further monitors and checks the IP & MAC address using the existing network tracking system to trace down the perpetrator.

E. Relocation Request

Figure 6 illustrates how to handle the relocation of the digital content request. There is always a possibility that genuine buyer may change the geographical location or the computer or the working and storing device. In such cases all the purchases will have to be surrendered to CA at transaction (1) with the new MAC address, to relocate to new device or location. Newly embedded digital content will be send to B in the transaction (2); which will be later forwarded to transaction (3).

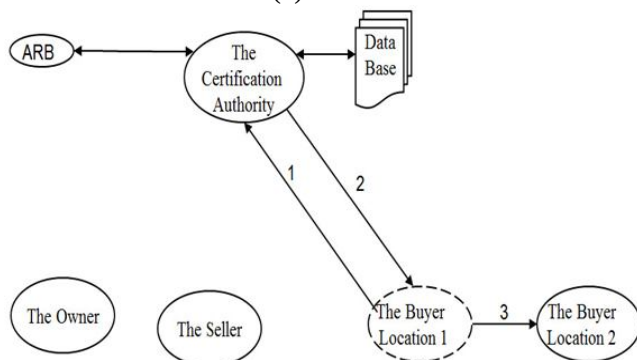


Fig 6 Relocation Request

Since the O and ARB gets the alert as soon as piracy observed, a proactive action and prevention against duplication, which will ultimately lead to copyright protection.

III. CONCLUSION

This paper proposed an efficient and secure buyer-seller watermarking protocol to identify the Perpetrator who actually pirates the digital content. All the existing system can be implemented in layer 3 of watermarking to solve the existing many issues stated by other researched in this field. The system is designed for any public key crypto system to restrict the unauthorized data drift. The security of this protocol lies on the efficient algorithm of TSR scripting program and flag counters. The security and robustness of the encryption standard and different homomorphism, permutation and combination functions used in this protocol also plays an important role, which can further be modified and developed to improve the efficiency of the protocol.

REFERENCES

- [1] Poh, G.S., Martin, K.M, "A framework for design and analysis of asymmetric fingerprinting protocols", Third International Symposium on Information Assurance and Security, pp. 457-461 (2007)
- [2] N Memon and P W Wong, "Protecting Digital Media Contents," Commun. ACM, Vol 41, No. 7, July 1998, pp. 35-43.
- [3] N Memon and P W Wong, "A Buyer-Seller Watermarking Protocol," IEEE Trans. on Image Processing, Vol. 10, Apr. 2001, pp. 643-649.
- [4] L Qiao and K Nahrstedt, "Watermarking Schemes and Protocols for Protecting Rightful Ownership and Customer's Right," J. of Visual Communication and Image Representation, Vol. 9, Sept. 1998, pp. 194-210.
- [5] Shao, M.H.: A privacy-preserving buyer-seller watermarking protocol with semi trust third party", Proceeding of TrustBus'07, Volume 4657, Springer LNCS, page 44-53., (2007)
- [6] Lei C-L, Yu P-L, Tsai P-L and Chan M-H, "An Efficient and Anonymous Buyer-Seller Watermarking Protocol," IEEE Trans. on Image Processing, Vol. 13, No.12, 2004, pp. 1618-1626.
- [7] Vinu V Das and NussyThankachan, "A Buyer-Seller Watermarking Protocol for an Efficient and Secure Digital Transaction," in Proc. 1st Int. Conf. on Information System and Technology, India, 2007, pp. 127-132.
- [8] K Gopalakrishnan, N Memon, and PL Vora, "Protocols for Watermark Verification," IEEE Multimedia, Vol. 8, Oct-Dec 2001, pp. 66-70.
- [9] J Zhang, WKou and K Fan, "Secure Buyer-Seller Watermarking Protocol," IEE Proc. Int. Conf. Security, Vol. 153, No. 1, March 2006.
- [10] Vinu V Das, "A Tree Based Buyer-Seller Watermarking Protocol," in Proc. 3rd Int. Joint Conf. on Computer, Information, Systems Sciences, and Engineering, USA, 2007.
- [11] Goi B-M, Phon R C-W, Yang Y, Bao F, Deng R H, and Siddiqi M U, "Cryptanalysis of two Anonymous Buyer-Seller Watermarking Protocols and an Improvement for true Anonymity," in Proc. Applied Cryptography and Network Security, 2004, LNCS 3089, pp. 369-382.
- [12] I M Ibrahim, SherifHazem N E-D, and Abdel Fatah A H, "An Effective and Secure Buyer-Seller Watermarking Protocol," IEEE Proc. 3rd Int. Symposium of Information Assurance and Security, 2007, pp. 21-26.
- [13] Chang C-C and Chung C-Y, "An Enhanced Buyer Seller Watermarking Protocol," in Proc. of ICCT 2003, IEEE CS Press, 2003, pp. 1779-1783.
- [14] Williams, DM, Treharne, H, Ho, AT Sand Culnane, C, "Using a Formal Analysis Technique to Identify an Unbinding Attack on a Buyer-Seller Watermarking Protocol", ACM Multimedia and Security Workshop, 2008